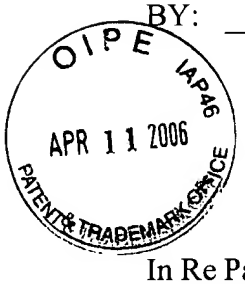
I HEREBY CERTIFY THAT THIS CORRESPONDENCE IS BEING DEPOSITED WITH THE UNITED STATES POSTAL SERVICE AS FIRST CLASS MAIL IN AN ENVELOPE ADDRESSED TO: COMMISSIONER FOR PATENTS, P.O. BOX 1450, ALEXANDRIA, VA 22313-1450, ON THE DATE INDICATED BELOW.

BY: Gladys G. Morales Date: April 4, 2006



MAIL STOP AMENDMENT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Patent Application of: Adam R. Schran et al.			
Conf. No.:	3079	Group Art Unit:	2161
Appln. No.:	09/820,054	Examiner:	Etienne Pierre Leroux
Filing Date:	March 28, 2001	Attorney Docket No.:	10397-1U1
Title:	SYSTEM AND METHOD FOR NETWORK ADMINISTRATION AND LOCAL ADMINISTRATION OF PRIVACY PROTECTION CRITERIA		

DECLARATION OF PRIOR INVENTION TO OVERCOME CITED PATENT (37 CFR § 1.131)

PURPOSE OF DECLARATION

This declaration is being submitted to establish completion of the invention in this application in the United States at a date prior to October 20, 2000, which is the earliest possible effective date of the prior art U.S. Patent Application Publication No. 2002/0055912 (Buck), which was cited and applied by the Examiner in an Office Action dated November 18, 2005.

The persons making this declaration are the inventors, and are thus qualified to submit this declaration under 37 CFR § 1.131.

FACTS AND DOCUMENTARY EVIDENCE

To establish the date of completion of the invention of this patent application, copies of the following documents and supporting statements are submitted as evidence:

Documents

EXHIBIT 1: Screen shot printout of a file folder that contains the executable code (.exe) of a beta version of ActivePrivacy.

EXHIBIT 2: Document entitled "INTELLECTUAL PROPERTY NEEDS ASSESSMENT" which provides an overview of the technical capabilities of ActivePrivacy.

EXHIBIT 3: Patentability search memorandum.

EXHIBIT 4: Email from a customer of ActivePrivacy.

EXHIBIT 5: Chart of independent claim limitations that shows documentation for each claim limitation.

Supporting statements

1. The blacked out dates labeled as D1-D4[1] in Exhibit 1 are all prior to October 20, 2000.

2. The blacked out date labeled D1 in Exhibit 2 is prior to October 20, 2000.

3. The blacked out dates labeled D1 and D2 in Exhibit 3 are both prior to October 20, 2000.

4. The blacked out dates labeled D1 and D2 in Exhibit 4 are both prior to October 20, 2000.

5. Each claim limitation in Exhibit 5 is supported by documentation that is dated prior to October 20, 2000. Text portions T1-T6 (there is no T2) referred to in Exhibit 5 correspond to respectively labeled text portions in Exhibits 2 and 3.

6. A beta version of ActivePrivacy was created and released prior to October 20, 2000, as evidenced by Exhibits 1 and 2. See, text portion T7 of Exhibit 2.

7. A commercial subscription-based version of ActivePrivacy was released and made available for a license fee prior to October 20, 2000, as evidenced by Exhibit 4.

[1] D4 refers only to the 272 kB ActivePrivacy.exe file.

8. The beta and commercial version of ActivePrivacy both contained all of the functionality of the claim limitations shown in Exhibit 5. General descriptions of such functionality are given in Exhibits 2 and 3.

9. ActivePrivacy is the commercial name of a software product associated with the presently claimed invention, as further evidenced by Figs. 4 and 6 of the present invention which show screen shots labeled with "ActivePrivacy."

From the attached documents and the supporting statements, we submit that it has been established that the invention in this application was made prior to October 20, 2000, which is the earliest possible effective date.

TIME OF PRESENTATION OF THE DECLARATION

This declaration is submitted prior to final rejection.

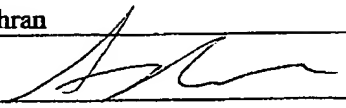
DECLARATION

As a person signing below:

I hereby declare that all statements made herein of my own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under Section 1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

SIGNATURES

Full name of first or sole inventor: Adam R. Schran

Inventor's Signature: 

Date: 4/5/2006

Residence: Philadelphia, Pennsylvania

Citizenship: United States of America

Post Office Address: 217 Church St #4 Phila PA 19147

Full name of second joint inventor: Robert E. Darlington

Inventor's Signature

Date

Residence: Los Alamos, New Mexico

Citizenship: United States of America

Post Office Address: 3260-B Orange Street, Los Alamos, New Mexico 87544

SIGNATURES

Full name of first or sole inventor: Adam R. Schran

Inventor's Signature: _____

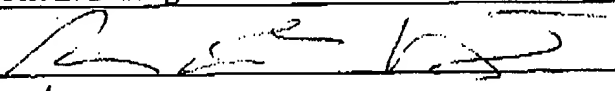
Date: _____

Residence: Philadelphia, Pennsylvania

Citizenship: United States of America

Post Office Address: _____

Full name of second joint inventor: Robert E. Darlington

Inventor's Signature: 

Date: 4/6/06

Residence: Los Alamos, New Mexico

Citizenship: United States of America

Post Office Address: 3260-B Orange Street, Los Alamos, New Mexico 87544

EXHIBIT 1 of "Declaration of Prior Invention…"
(Application No. 09/820,054)

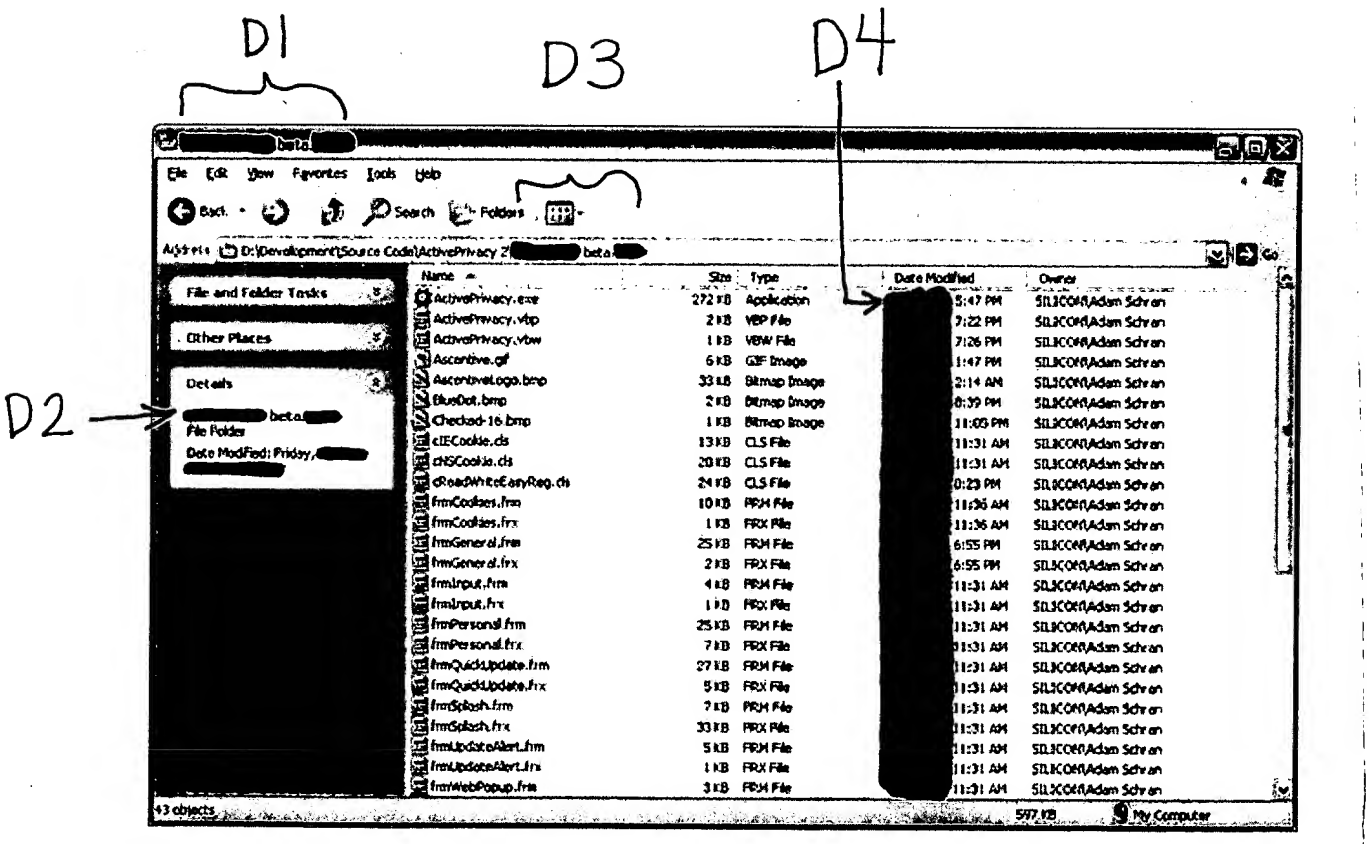


EXHIBIT 2 of "Declaration of Prior Invention..."
(Application No. 09/820,054)

D1 { [redacted]

INTELLECTUAL PROPERTY NEEDS ASSESSMENT

Ascentive

Adam Schran

Introduction
Ascentive, an Internet software company, was founded in November 1998 on the proverbial 'back of the napkin' and launched in January 1999. Since then, revenue has grown at an average 50% per month, resulting from a successful focus on building a network of 3,000+ affiliate web sites to bootstrap the company.

Products
Since launch, Ascentive has brought to market two consumer software products for Windows:

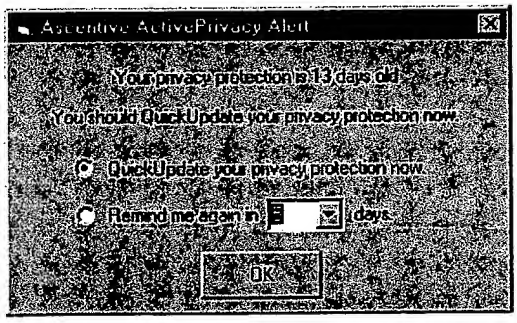
- WebROCKET Internet Optimizer – An instant speed boost for any dial-up or high-speed Internet connection.
- WinROCKET Computer Optimizer – Performance booster for all computers running Windows 95 and 98.

ActivePrivacy Overview T7
ActivePrivacy, currently undergoing beta testing, represents a leap forward in privacy protection from the current tools-driven convention to a service-driven model.

In the current schema, Internet users have one of three options:

- Head in the sand: Do nothing about potential privacy violations.
- Scorched earth: Disable all avenues for privacy violations, thus reducing the utility and automation of many web sites.
- Do it yourself: Scan for potential privacy violations yourself, consuming time and energy.

ActivePrivacy's service approach is superior to all three methods.



T1 {

- Customer subscribes to the ActivePrivacy QuickUpdate privacy service to manage their privacy needs. The QuickUpdate service includes the latest privacy protection, consisting of a "Watchlist" of sites that use cookie files to store unique or identifying information.

T3 {

- ActivePrivacy, the client software, scans for privacy violations and takes corrective action while you use the Internet. To trigger potential privacy violations, the Watchlist (retrieved by the client software from Ascentive's QuickUpdate server) is merged with the end user's Blacklist, exempting any sites in the end user's Trustlist.

T6 {

T5

T4

- The end user is reminded to keep their Watchlist up to date by QuickUpdating frequently.

Inventions
We believe the following innovations in ActivePrivacy are new and non-obvious, and are good candidates for patent protection.

- Determing and taking corrective action for privacy violations that have already occurred by merging "QuickUpdate" Watchlist privacy protection with the end-user's Blacklist and Trustlist.
- "Privacy safe browsing", a browser window in the client/server that uses the QuickUpdate privacy protection to preemptively strike against privacy violations.
- The ActivePrivacy QuickUpdate server, a system that distributes incremental updates to end users' privacy protection through the QuickUpdate client software.

EXHIBIT 3 of "Declaration of Prior Invention..."
(Application No. 09/820,054)

AKIN, GUMP, STRAUSS, HAUER & FELD, L.L.P.

ATTORNEYS AT LAW
One Commerce Square - 2005 Market Street - Suite 2200
PHILADELPHIA, PA 19103-7086
Telephone: (215) 965-1200 - FAX: (215) 965-1210
E-MAIL: &@@akingump.com

CONFIDENTIAL D1→ [redacted] **CONFIDENTI**

VIA FACSIMILE: 703-415- 1017 - (Confirmation copy via First-Class Mail)

SEARCHER: Randy Lacasse **Client No.:**

210397.0001

FROM: Louis Sickles **PAGE 1 OF 4** **DEADLINE:**

D2→ [redacted]

( ) Telephone Confirmation (X) New Instructions ( ) Fax Confirmation

INSTRUCTIONS: ( ) Detailed Instructions Attac

Please conduct a patentability search on a regular basis for a Method of Expunging Unwanted Cookies from a Computer.

A "cookie" is a short piece of data which is transmitted from certain Internet hypertext transfer protocol (HTTP) server computers to a client computer when the HTTP server connects to the client computer in response to a uniform resource locator (URL) request from the client computer. The cookie includes, in part, data related to the web page accessed by the client computer and the domain attributes of the server. Cookies transmitted from individual server computers are separately stored in the memory of the client computer.

In subsequent transactions between the client computer and a server which had previously transmitted a cookie to the client computer, (or a server included in the domain specified by the server), a copy of the cookie stored in the client computer and linked to that domain address is automatically included in the client computer's URL request. In this way, the server receiving the URL request knows that the user has previously connected to the server and can (if desired) direct the client's access to a specific page (or pages) on its web site.

Cookies are typically used by Internet shopping sites to keep track of the user's shopping cart. When a user first visits an Internet shopping site, the user is sent a cookie containing the name (ID number) of a shopping cart. Each time an item is selected for purchase, the shopping site correlates that selection to the shopping cart by the shopping cart ID number

contained in the cookie and adds the selection to the cookie. When the user is done with shopping, the checkout page lists all of the items in the shopping cart tied to the cookie. Without cookies, the user would have to keep track of all the items that the user wanted to buy and type them into the checkout page at the conclusion of the transaction, or buy each item one at a time. Alternative to accumulating the shopping cart data in a single cookie, the shopping site could send a separate cookie containing the selected item number to the client computer whenever an item was selected to purchase.

One of the less admirable and controversial uses of cookies is for tracking the browsing and buying habits of individual web users. On a single web site or a group of web sites within a single sub-domain, cookies can be used to see what web pages the user visits and how often the user visits them. On web sites which display banner advertisements from a single marketing site, cookies can be used to track the browsing habits on all of the web sites being serviced by the marketing site. Tracking is accomplished by issuing a cookie with the marketing site's domain specified when the user clicks on the advertisement. Subsequent connection of a user to any web site displaying one of the marketing site's advertisements results in a cookie being sent to the marketing site. The marketing site can correlate the users buying habits from the plurality of cookies and develop a profile of the user.

Currently, a user has only two options if the user prefers not to have his web browsing habits tracked. Commercial browsers, (e.g.. Internet Explorer or Netscape Navigator), provide options that: (1) prevent any cookie from being stored in the user's computer, (2) notify the user each time a cookie is sent to the browser allowing the user to reject or accept the cookie, or (3) accept all cookies. None of the aforementioned options is entirely satisfactorily. In the first case, the user will be prevented from connecting with many desirable sites that do not abuse the use of the cookie. In the second case, the user will be likely be annoyed by the notification messages which may occur numerous times during a connection to a single web site.

Software applications are known which can be installed in a client computer to give the user additional control over cookies. These software packages typically allow the user to accept, reject or delete cookies from the client computer that originate from user specified web sites. However, all of these known software packages require the user to develop the list of unwanted web sites.

In the proposed system concept an HTTP server maintains a watch list of Internet sites that use cookies to store unique or identifying information about a user. The user's computer contains both a user developed black list of Internet sites for which the user prefers not to have cookies stored in his system, and a user developed list of trusted Internet sites for which the user has perfect trust. In use, the user is periodically prompted to connect the client computer with the HTTP server containing the watch list. In response, the HTTP server downloads the watch list to the user's computer. The watch list is combined with the user's blacklist and the user's trusted list to create a composite list of Internet sites. The composite list is formed by subtracting sites on the trusted list from the watch list and adding the result to the user's black list.

The user's software can operate in two different modes. In the first mode, the user's software deletes offending cookies from the user's memory based on the composite list. In this mode, the user may set the software to execute at any periodicity he chooses, from seconds to hours. In the second mode, the software operates continuously to intercept cookies as the cookies are received from the offending web server. The watch list may also include attributes that characterize the Internet sites using cookies based on the degree of identifying information contained in the cookie. In these instances, the user would be notified that the cookie was present in his system or is being sent to the system and the user would be given the option of editing the composite list to accept or reject cookies from that site.

Note that a similar concept is used to download anti-virus software to client computers. However, the concept of the present invention differs in at least two respects: (1) the combining of the watch list, the black list and the trusted list and (2) the concept of detecting and rejecting the cookie as it is received by the user's computer.

The following words and phrases are sometimes usd synnomynously for cookies and may assist in searching for references related to "cookies": persistent cookie; token; state object; and state management.

In summary, please focus your search on the following concepts: (1) a computer software program residing in a server computer that maintains a watch list of computer servers that use cookies to store unique or identifying information about a user and upon request downloads the watch list to a subscribing client computer; and (2) a computer program that resides in a subscribing client computer that maintains a black list and a trusted list and uses the

black list and the trusted list in conjunction with the downloaded watch list to either delete unwanted cookies from the client computer memory and/or reject unwanted cookies as they are received in the client computer.

If you require additional information please contact me at the above 215-965-1294.

Thank you.

FOR SEARCHER'S USE ONLY

Date Completed: _____
Time: _____
Costs: _____

EXHIBIT 4 of "Declaration of Prior Invention..."
(Application No. 09/820,054)

D1

CSNavy@aol.com, 01:53 AM [redacted], Active Privacy Problem

D2

From: CSNavy@aol.com
Date: Sat, [redacted] 02:53:25 EDT
Subject: Active Privacy Problem
To: comments@ascentive.com
X-Mailer: AOL 5.0 for Windows sub 119

Dear Sir Or Madam:
After the first few days of using ActivePrivacy I've been unable to keep the program running on my computer. After 20 minutes to 1 hour a window pops up with Run error Division by zero and the program shuts down once this is acknowledged.
This makes the ActivePrivacy program virtually useless to me. Unless I can find a solution to this I will discontinue using it and uninstall this program.

V/R
Kelsey Baker

EXHIBIT 5 of "Declaration of Prior Invention..."
(Application No. 09/820,054)

Chart of independent claim limitations that shows documentation for each claim limitation

Text of independent claims	Exhibit(s) that support claim limitations
1. A method of screening cookie files in a client machine, the method comprising:	
(a) receiving, at a server, a request from a subscriber to send a list of cookie file sources to the client machine;	Exhibit 2: T1 Exhibit 3: T1
(b) downloading the list from the server to the client machine; and	Exhibit 2: T1 Exhibit 3: T1
(c) using the downloaded list to detect cookie files received at the client machine from sources on the downloaded list.	Exhibit 2: T3 Exhibit 3: T3
16.	Same as claim 1

Text of independent claims	Exhibit(s) that support claim limitations
7. A method of creating a composite list of cookie file sources in a client machine, the method comprising:	
(a) creating a first exception list including the identity of sources that are permitted to store cookie files in the client machine;	Exhibit 2: T4 Exhibit 3: T4
(b) creating a second exception list including the identity of sources that are not permitted to store cookie files in the client machine;	Exhibit 2: T5 Exhibit 3: T5
(c) receiving at the client machine, from a service provider, a master list of cookie file sources; and	Exhibit 2: T1 Exhibit 3: T1
(d) modifying the master list in accordance with the first and second exception lists, wherein the composite list is the modified master list.	Exhibit 2: T6 Exhibit 3: T6
22.	Same as claim 7

Text of independent claims	Exhibit(s) that support claim limitations
12. A method of creating a composite list of cookie file sources in a client machine, the method comprising:	
(a) receiving at the client machine, from a service provider, a master list of cookie file sources;	Exhibit 2: T1 Exhibit 3: T1
(b) deleting cookie file sources from the master list that correspond to one or more trusted cookie file sources listed in the client machine; and	Exhibit 2: T4, T6 Exhibit 3: T4, T6
(c) adding cookie file sources to the master list that correspond to one or more untrusted cookie file sources listed in the client machine, wherein the composite list is the master list as modified by any additions and deletions of trusted and untrusted cookie file sources.	Exhibit 2: T5, T6 Exhibit 3: T5, T6
27.	Same as claim 12